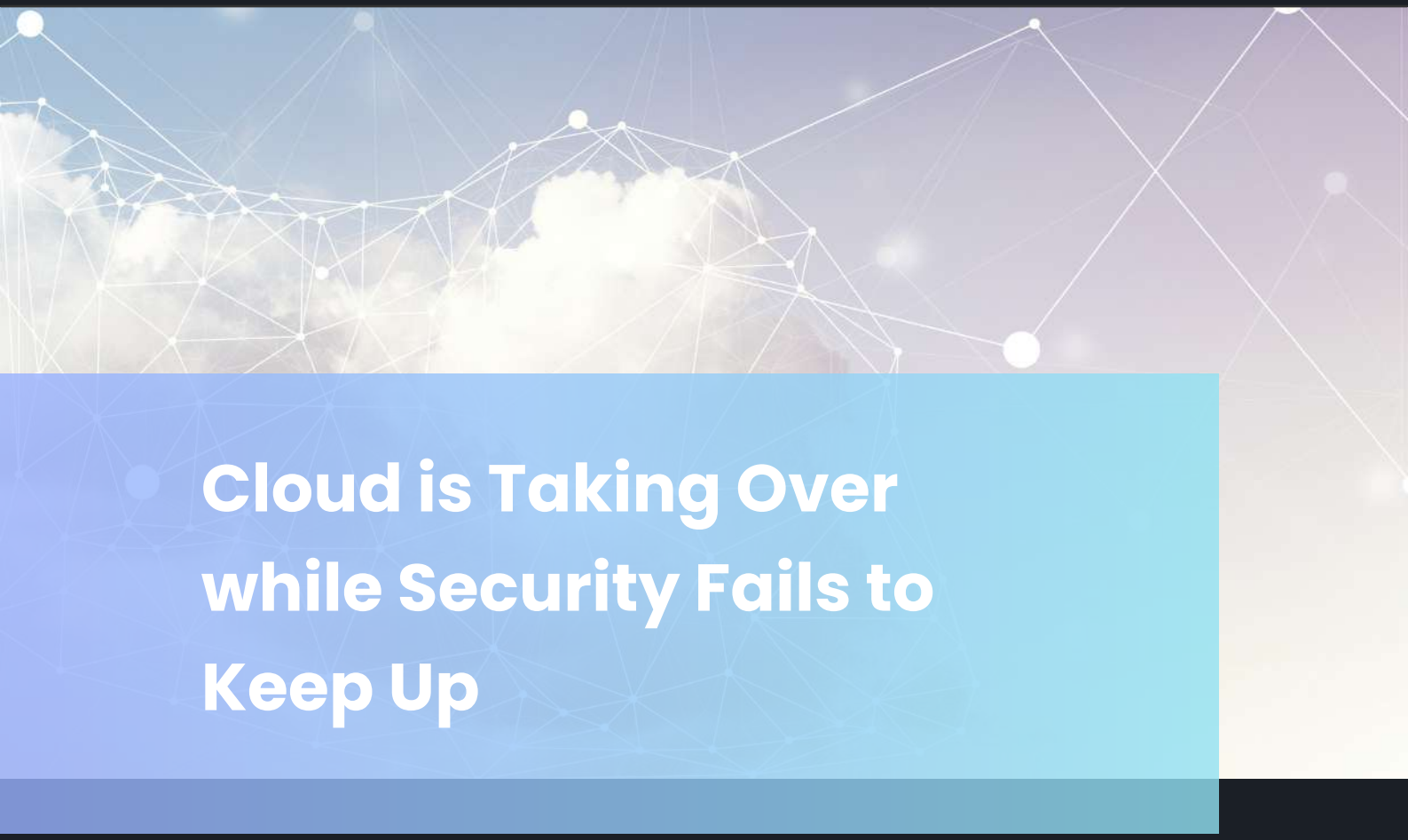
WHITE PAPER

Untangling Secure Access

Peig



Cloud is Taking Over while Security Fails to Keep Up

Cloud productivity services focus on being best at one thing rather than being mediocre at everything – a winning business strategy. Organizations take advantage of several specialized single-purpose services that solve individual business problems exceptionally well. As a side-effect, **managing identity & access security in a fragmented service environment is proving difficult.** To make things worse, with a growing dependency on cloud services[1] cyber threats are rising steadily. Leading the way in successful cyberattacks, hackers take advantage of human error and identity theft to profit from accessing sensitive data.

In battling identity theft, state-of-the-art identity and access management have grown beyond coherence. **The industry has evolved around a plethora of vague techy solutions, where each one is a remedy for another:** *Where passwords are not enough, use Multi-Factor Authentication! When MFA hinges productivity, use SSO! When SSO becomes too risky, add adaptive authentication!*

Such a card house approach to access security is no longer viable: For businesses, cyber threats have reached a point of mainstream existential risk – common cyberattacks lead to significant financial loss, customer trust decline, and/or bankruptcy.
Untangling access security demands a full-stack access service that eliminates fundamental identity flaws at the core.

Peig introduces an identity-first approach that closes the identity gap and removes the most prominent cyber threats by design. In doing so, organizations increase their access control security confidence to a point that no longer requires layers of technical compromises. Human-centred by design, Peig makes sure end users never struggle with authentication fatigue and organizations face no downtime while keeping access security under control.

Identity & Access Management Legacy

The cost of a growing business

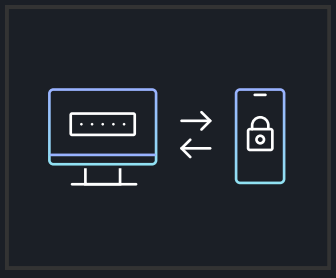
Coordinating access security responsibly can be challenging. **With more SaaS tools and people to manage, companies face difficulties managing who can access what.** This is hardly surprising given the broad range of siloed applications – each being used by different people in the company, each providing proprietary ways to manage users and subscriptions, and finally, each having different access security designs. With freelancers and external teams jumping on and off applications for individual projects in real-time, teams have a hard time onboarding, managing, or offboarding users in ways that are practical and simultaneously keep their data safe.

This scattered approach is damaging team productivity - onboarding team members is often done in uncoordinated ways and takes precious time of everyone involved. In addition, **the growing demand for remote work and BYOD makes secure user onboarding more costly and increasingly difficult to manage.**

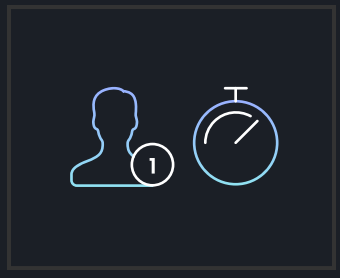
Password & MFA fatigue

- Typing passwords and using multi-factor authentication takes time. For MFA to have the proper security effect, **authentication can take over 9 employee hours a year spent just dealing with authentication requests.**
- Dealing with passwords and multi-factor authenticators is distracting – studies show that **authentication disturbances increase stress, hinder focus and, as a result, reduce the quality of work**, which further reduces the effectiveness of MFA security.
- **Password resets, or MFA device loss** puts work to a halt. Forgetting passwords and misplacing authenticators **typically result in not having access for hours or even days**. Organizations not only lose valuable time but can suffer indirect damages during downtime, e.g. lost prospects or violating contract terms.

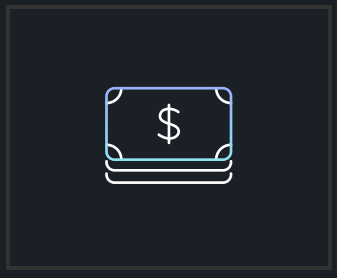
252 x
YEARLY AUTHENTICATIONS



9.8 hours
AUTHENTICATING PER EMPLOYEE



30.340 USD
LOST PER EVERY 100 EMPLOYEES



Rising cyber risks

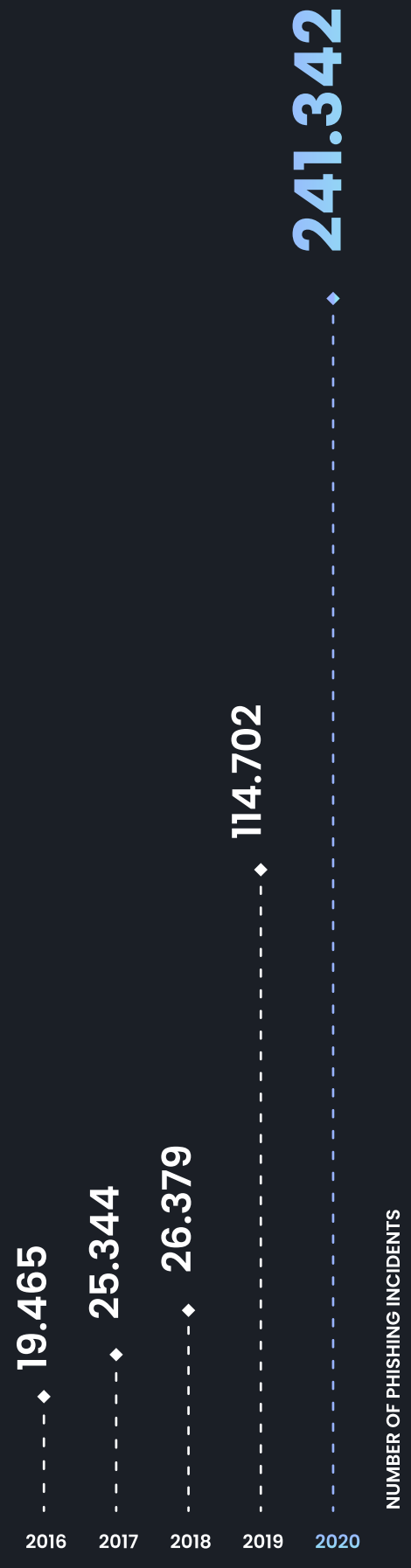
Cyber risks are imminent for rising start-ups, SMBs, as well as enterprises. According to the FBI, **phishing attacks were the most common form of cybercrime, with 241,324 incidents in 2020 - more than double compared to 2019.**[2] 30% were targeted at smaller to medium sized businesses.

According to a 2020 Trend Macro Report, **74% of all phishing websites used the HTTPS protocol.**[3] With an HTTPS green certificate dominating the phishing threat space, end-users and organizations have no practical way of detecting phishing websites. Green certificates no longer provide the intended identity & access security – instead, they give a false impression of trust in attackers' websites.

According to Hashed Out, a staggering **95% of all HTTPS servers are vulnerable to MitM attacks.**[4] The same report also shows that **MitM attacks accounted for nearly 35% of all security incidences in 2019.**

With rising cyber threats, there is a need for stronger and more granular access security. Frequent resource-specific access verification and enforcement are needed to face concurrent threat challenges (*as a side-effect, this also deepens the hidden cost of traditional MFA on productivity and employee stress*).

Passwords and most multi-factor authenticators cannot stop phishing and MitM attacks. In the past, phishing scams were mostly targeted at systems with only password protection; however, with the rise of MFA in businesses, hackers have professionalized methods of MFA spear phishing.



Cost of traditional access management

Access management solutions are typically affordable to buy, deploy and technically maintain. Unfortunately, there are also undesirable side costs which include:

- Technical support for **user and device onboarding.**
- Service desk and IT support costs to accommodate for **password and lost authenticator access recovery** and **unwanted workforce downtime.**
- **Additional subscription costs** by SaaS providers who seek profit on access management and security.

Access security is entangled

Trapped in legacy, access management vendors offer portfolios of double-edged solutions. Single Sign-On, Multi-Factor Authentication, Adaptive MFA or notification-based Passwordless are some common methods that attempt to improve the reliability of username and password-based access security.

Single Sign-on (SSO)

⊕ Increases user convenience by providing a single set of credentials.
⊕ Increases usability with session cookies that don't require repeated authentication.
⊖ Increases risk by centralizing access security in a single point of failure.
⊖ Significantly reduces security confidence: session cookies = common point of exploit.

Multi-factor Authentication (MFA)

⊕ Increases security because real users are required to confirm authentication with an additional device-bound factor.
⊖ Reduced user experience since users must take additional steps.
⊖ Dependency on an additional device.
⊖ Hard recovery in the case of loss.

Adaptive MFA

⊕ Reduces the number of times MFA is required.
⊖ Based on behavior analytics - attackers learn to forge behavior.
⊖ In critical situations, adaptive MFA further undermines the effort to recover.

Traditional Passwordless

⊕ No need for passwords, which are hard to remember and manage.
⊖ Doesn’t help with modern MFA phishing vulnerabilities.
⊖ Users still need an additional device - that is slow to use.

Building security improvements of a legacy approach to access security proves to diminish reliability and utility. The username & password as a foundation for secure access results in layers of technical compromise.

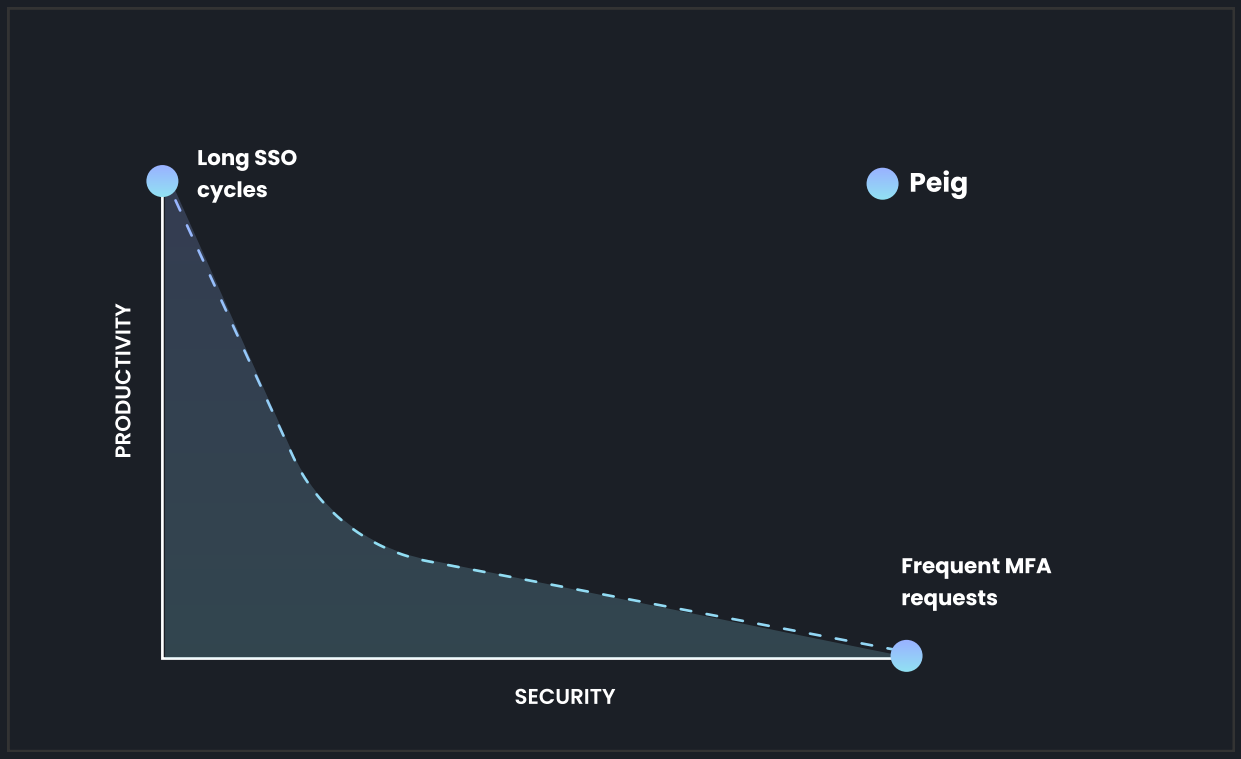
Full-Stack Access Platform

Peig Access Platform replaces the username (and related password) as a foundation of concurrent identity-based access control. In doing so, Peig manages to:

- **Undermine critical vulnerabilities** including spear phishing, MFA phishing, MitM, session hijacking, dictionary attacks, or brute-force attacks by closing the authentication gap.
- **Eliminate the need for additional HW tokens** or dependency on smartphone authenticators when working on desktop.
- **Reduce time spent on user authentication** and reduce **effects of authentication fatigue**.
- **Diminish downtime** in user or device **onboarding** scenarios.
- **Eliminate adaptive authentication downtime** in extraordinary user situations.
- **Simplify access** and security policy obstacles to a minimum.
- Deliver **integration flexibility** to eliminate adoption barriers.
- **Enforce reliable Zero Trust** in private/public cloud or physical server scenarios.

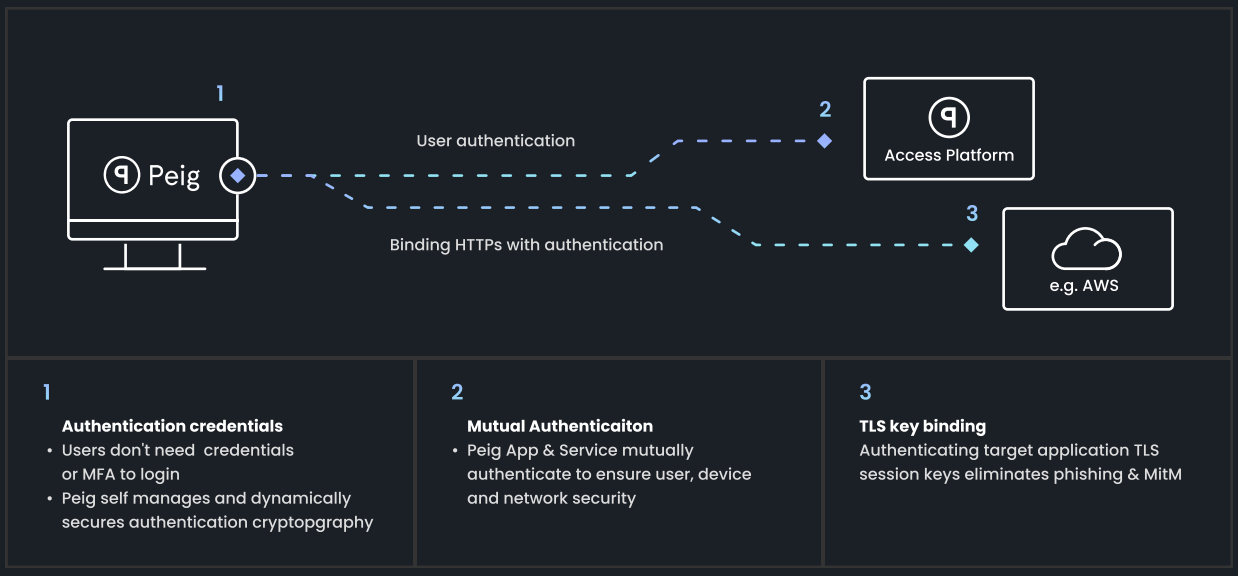
Untangling access compromise

Peig eliminates the need to balance security and convenience. Access security is no longer a question of intricate and case-specific risk assessment. Secure by-default Peig always maximizes both usability and cybersecurity.



The Peig Access Platform architecture is built on automated identifier and cryptography management. Users are not exposed to credential usage and management. As a result, employees are not required to undergo security training and practice a strict security policy that leaves room for human error. Security policy often expects unrealistic behavior, including periodically changing and remembering long passwords or spotting MFA spear-phishing emails. Peig security measures instead rely on advanced cryptography management and reliable automated authentication algorithms under the roof.

The vast majority of identity-related cybercrime results from underperforming access security online**. Login credentials and MFA must be replaced by much stronger and more dynamic counterparts**. Taking full advantage of our devices' computing power, Peig is based on reliable cryptography, mutual authentication, TLS session binding and end-point cryptography security.



1

Authentication credentials

- Users don't need credentials or MFA to login
- Peig self manages and dynamically secures authentication cryptopgraphy

2

Mutual Authenticaiton

- Peig App & Service mutually authenticate to ensure user, device and network security

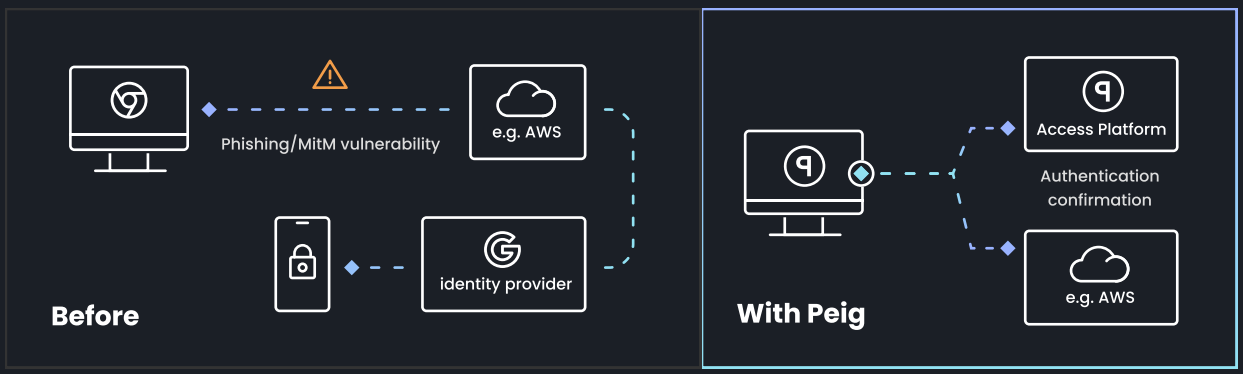
3

TLS key binding

Authenticating target application TLS session keys eliminates phishing & MitM

Fixing green certificate HTTPS security

Fixing access security requires fully closing the gap between session channels and authentication. Up to today, authentication security rarely had anything to do with session security. MFA apps authenticate users in a separate channel and hope for the best. This insufficient approach is an open door to phishing & MitM attacks. Peig closes the gap by using the full potential of HTTPS. **The architecture combines Peig cryptography to authenticate TLS keys on both Transport Layer ends. In doing this, Peig re-established trust in "green certificates" and standard TLS encryption.**



Dynamic end-point security

HW-based key protection is no longer plausible for access protection. HW tokens are difficult to distribute and manage over time resulting in undesirable downtime in case of loss or malfunction. On the other hand, cryptographic data used for access security needs to be well protected. To ensure access key security, Peig uses layers of periodical mutual verifications to ensure Peig cryptography hasn't been tampered with and to offer additional malware protection. In case security keys are moved or misused, Peig detects an end-point attack attempt.

Productivity & user experience

Peig design minimizes user verification interaction to invisible. Users no longer need to type passwords, pull out their phone for authentication requests or use HW tokens to work in a top security environment. Users access company services directly from Peig just like they would from any browser because Peig is built on Google's Chromium browser to make the experience 100% familiar while adding unprecedented levels of security that end users don't need to worry about.

- Save time authenticating
- Eliminate authentication fatigue
- Reduce employee stress

Instant onboarding

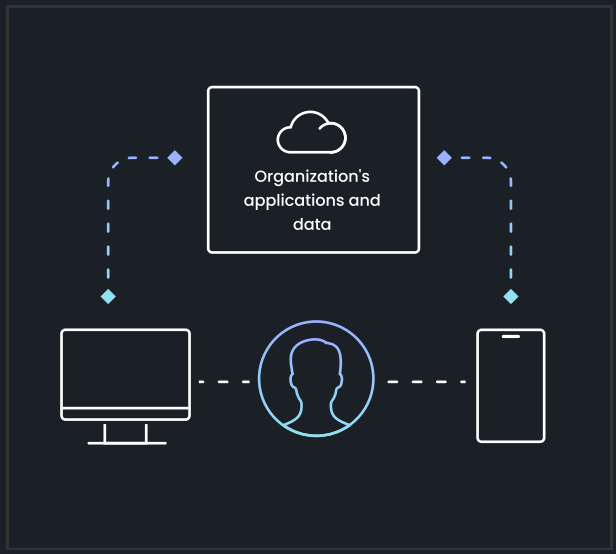
To eliminate downtime and lengthy onboarding processes, Peig takes full advantage of facial recognition and remote identity verification tech. Employees can onboard remotely without technical support or HR help. A self-service process has them do an ID document scan and a selfie to verify their identity, which has them fully onboarded. In doing so, authorized employees gain access to appropriate enterprise resources. From this point, repeated user verification is invisible to the end user.

Trusted employees can also help onboard new teammates when appropriate by other supported types of quick and secure onboarding processes.

- Onboard new teammates instantly
- Reduce/eliminate downtime due to device loss, etc.
- Work fully remote

One device & any device

Working remote is possible on all employee's devices. **Employees always only need the one device that is right for the task at hand to access their organization's resources – access on one device is never dependent on the availability of the other to minimize unwanted downtime.** Employees may also onboard additional devices on their own to access company resources securely. In doing so, a desktop not only becomes an access point, but also a backup for an employee's smartphone in case of loss or malfunction. Devices are always in sync so that users can disable old or lost devices at any time. User and device onboarding is always a matter of minutes.

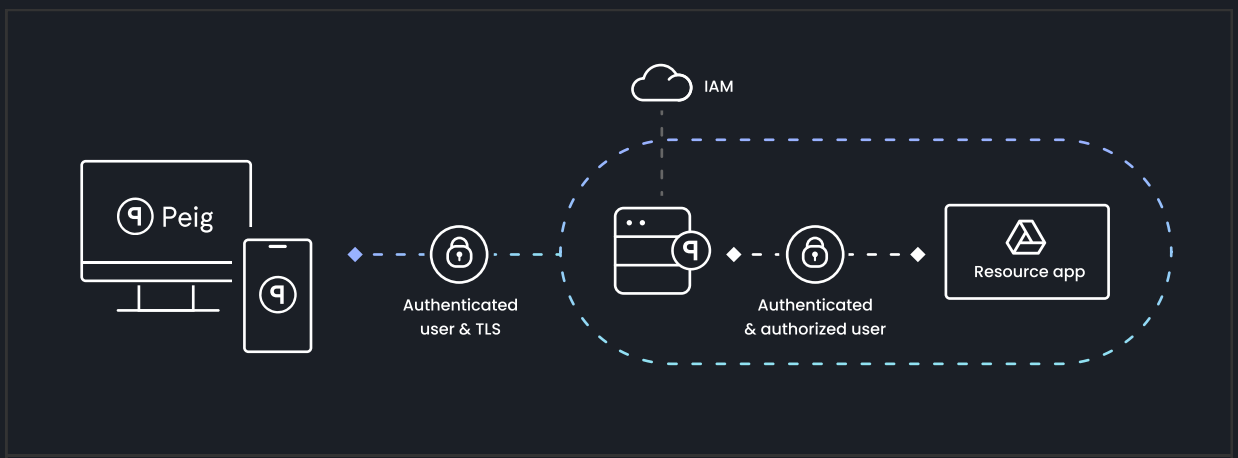


Workspace in Zero Trust

Once onboarded, employees can immediately access only applications and resources in the workspace for which they have been authorized. Leaving perimeter security behind, resources are independently protected, respecting Zero Trust security methodology.

Private-cloud and on-premises resources may each have an independent policy enforcement point, which are all centrally managed.

Access rights are consistently immediately enforced to maximize control over who can access what at what time. In doing so, employees access the minimum number of sensitive resources and for minimal time periods. Unauthorized access security risks are minimized as a result.



Private cloud & on-premise workspace in Zero Trust

Offering a whole new concept of enterprise data security, Peig Access Platform is a unique Zero Trust solution for all businesses, from SMEs to Fortune 500 companies. Like a finely tuned race car, Peig is built for peak performance with all required safety and security hidden away with no compromises made. Each second not spent navigating outdated security procedures is a second spent building up your company. SaaS applications, private cloud, or hybrid deployments, Peig Access Platform is designed to be easily integrated and utilized with any number of business applications.

REFERENCES

1) "Cloud Computing Market | Market Share, Size, & Growth 2021," accessed September 21, 2021, https://www.datamation.com/cloud/cloud-computing-market/

2) "IC3 Releases 2020 Internet Crime Report," Press Release, Federal Bureau of Investigation, accessed September 23, 2021, https://www.fbi.gov/news/pressrel/press-releases/fbi-releases the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam statistics.

3) Casey Crane on April 22 and 2020, "Phishing Statistics: The 29 Latest Phishing Stats to Know in 2020," Security Boulevard (blog), April 22, 2020, https://securityboulevard.com/2020/04/phishing statistics-the-29-latest-phishing-stats-to-know-in-2020/.

4) "80 Eye-Opening Cyber Security Statistics for 2019," Hashed Out by The SSL StoreTM (blog), April 10, 2019, https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/